



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/090,718	03/04/2002	Martin Hurich	10191/2275	4797
26646	7590	11/15/2006	EXAMINER	
KENYON & KENYON LLP ONE BROADWAY NEW YORK, NY 10004			CERVETTI, DAVID GARCIA	
			ART UNIT	PAPER NUMBER
			2136	

DATE MAILED: 11/15/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

10/090,718

Applicant(s)

HURICH, MARTIN

Examiner

David G. Cervetti

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 25 August 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-16 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-16 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 04 March 2002 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. Applicant's arguments filed August 25, 2006, have been fully considered but they are not persuasive.
2. Claims 1-16 are pending and have been examined.

### *Response to Amendment*

3. The objections to the specification are withdrawn.
4. The rejection of claim 1 under 35 U.S.C. 112, second paragraph, is withdrawn.
5. Examiner respectfully submits that a hash function would perform the "no byte-wise allocation between input and output data occurs", since this simply means that if the input string is 2 bytes in length, the output string is not that length.
6. Kawano et al. (US Patent 5,995,623, hereinafter Kawano) teach encrypting information to be transmitted so that no byte-wise allocation between input and output data occurs (hashing). Kawano selects pieces of information to be encrypted, thus provides the architecture to perform the claimed invention.
7. Furthermore, stream ciphers applied to a "complete stream" were conventional and well known, as it was to apply hash functions to the encrypted content (Menezes et al., chapter 9, hereinafter Menezes).
8. Regarding Applicant's argument about Kawano, upon a further examination of the reference, Examiner submits that Kawano does in fact operate on a "complete stream of data", giving it the broadest reasonable interpretation consistent with the specification. Kawano operates on a message or input data. **Applicant's arguments are not persuasive.**

Art Unit: 2136

9. Even if the simplistic interpretation submitted by Applicant is accepted, i.e., that one skilled in the art would at most recognize two possible and mutually exclusive possibilities for performing encryption, there is no re-definition of what "complete" is, therefore, what Kawano hashes, encrypts, and sends, constitutes a "complete stream of data". **Applicant's arguments are not persuasive.**

10. Regarding Applicant's argument about "byte-wise allocation", Examiner respectfully submits that it is inherent to the inner working of a hash function/compression function/etc. A hash function maps larger domains to smaller ranges, more precisely, a hash function  $h$  maps bit strings of arbitrary finite length to strings of fixed length, say  $n$  bits, thus a byte-wise allocation does not occur (Menezes, chapter 9). **Applicant's arguments are not persuasive.**

***Continued Examination Under 37 CFR 1.114***

11. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.

***Claim Objections***

12. Claim 1 is objected to because of the following informalities: programming unit and control unit are used interchangeably. Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

13. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

14. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites the limitation "encrypted in the control unit". There is insufficient antecedent basis for this limitation in the claim.

***Claim Rejections - 35 USC § 102***

15. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

16. **Claims 1-16 are rejected under 35 U.S.C. 102(b) as being anticipated by Wasilewski et al. (US Patent 6,157,719, hereinafter Wasilewski).**

**Regarding claims 1, 7, 11, 13, 15, and 16, Wasilewski teaches a method of data encryption in programming of a control unit comprising:**

- encrypting a complete stream of data to be transmitted in a programming unit using a first key, wherein a byte by byte encryption of the complete stream of data is capable of being performed, and wherein no byte-wise allocation between input and output data occurs (col. 6, lines 16-55);

Art Unit: 2136

- transmitting the data that had been encrypted to the control unit via a data line (**col. 6, lines 56-67, col. 7, lines 1-25**); and
- decrypting the data that had been encrypted in the control unit using a second key provided in the control unit (**col. 7, lines 25-67**).

**Regarding claims 2 and 8**, Wasilewski teaches wherein the first key and the second key are identical (**col. 6, lines 16-55**).

**Regarding claims 3 and 9**, Wasilewski teaches wherein the first key and the second key are not identical (**col. 6, lines 16-55**).

**Regarding claim 4**, Wasilewski teaches wherein each one of the first key and the second key includes a table that is accessed by a hash function (**col. 8, lines 1-63**).

**Regarding claim 5**, Wasilewski teaches wherein at least one of the first key and the second key is implemented in an electronic circuit (**col. 8, lines 1-63**).

**Regarding claim 6**, Wasilewski teaches wherein at least one of the first key and the second key is implemented in the form of a computer program (**col. 8, lines 1-63**).

**Regarding claim 10**, Wasilewski teaches wherein the programming unit and the control unit each includes an electronic computing unit and a memory module that are linked together by a data bus (**fig. 2A, cols. 6-7**).

**Regarding claim 12**, Wasilewski teaches wherein the computing unit includes an electronic computing unit in a programming unit (**fig. 2A, cols. 6-7**).

**Regarding claim 14**, Wasilewski teaches wherein the computing unit includes an electronic computing unit in a control unit (**fig. 2A, cols. 6-7**).

### **Conclusion**

Art Unit: 2136

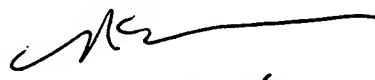
17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

18. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

19. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

DGC

NASSER MOAZZAMI  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100



11,13,06